STATEMENT

BY

Richard Campanelli, Director
Office for Civil Rights
U.S. Department of Health and Human Services

A Hearing Before The
Senate Special Committee on Aging

628 Dirksen
Senate Office Building
9:30 A.M.
September 23, 2003

Chairman Craig, Senator Breaux, distinguished members of the Committee, I welcome the opportunity to appear before you today to discuss the implementation of the Standards for Privacy

of Individually Identifiable Health Information (the Privacy Rule), adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). As the Director of the Office for Civil Rights (OCR), within the U.S. Department of Health and Human Services, I oversee the office that has responsibility for implementing, enforcing, and aiding covered entities to come into compliance with the Privacy Rule.

By way of background, Congress enacted HIPAA in 1996, among other things, to improve the efficiency and effectiveness of the health care system, through "administrative simplification" provisions that created a process for the establishment of standards and requirements for the electronic transmission of certain health information.[1] At the same time, Congress recognized that administrative simplification must be accompanied by protections for the privacy and confidentiality of personal health information, since, as a consequence of more efficient transmission of health information, private health information also would become more readily accessible. Therefore, in enacting HIPAA Congress directed that standards be developed to protect the security and privacy of health information,[2] and established civil and criminal penalties for various violations of those standards. Pursuant to Congress' mandate, HHS issued a proposed Privacy Rule in November 1999, received over 50,000 public comments, and published a final Privacy Rule in December of 2000. Because of continuing concern over aspects of the Rule, in February 2001, HHS announced that it would reopen the Rule for comments, and, after receiving thousands of comments, in April 2001 it proposed to issue recommended modifications to avoid the unintended consequences of the Privacy Rule and improve its workability. Those proposed modifications were published in April 2002, and received some 11,000 additional comments. Finally, just over a year ago, on August 14, 2002, HHS

---

[1]Sections 261 through 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, are known as the Administrative Simplification provisions.

[2]In the HIPAA statute, Congress gave itself a deadline for passing a privacy statute of August 21, 1999. Section 264(c)(1) of HIPAA provides that: "If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by [August 21, 1999], the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than [February 21, 2000]."

finalized those modifications to improve workability while maintaining strong privacy protections. As covered entities have known since the Rule took effect, most covered entities were required to comply with the Privacy Rule as of the April 14, 2003, with small health plans having an additional year to comply.

The Privacy Rule establishes the Nation's first-ever comprehensive standards for protecting the privacy of American's personal health records. As of April 14, 2003, patients have sweeping federal protections over the privacy of their medical records, rights to access and to correct errors in their medical records, rights to control how their protected health information is used and disclosed, and a clear avenue of recourse if the rights afforded by the Privacy Rule are violated.

We know that the Committee is particularly interested in our experience, and that of covered entities and consumers, with the Privacy Rule now that some five months have passed since April 14. Particularly, Committee staff have advised that the Committee desires to be apprised of any areas of confusion, or misconception, that have occurred after April 14, and how HHS is addressing those issues. Because a number of areas that have received public attention are significantly addressed by modifications to the rule made last August, I will focus on the nature and impact of these modifications, before turning to HHS efforts to promote understanding of and compliance with the Privacy Rule – and to dispel the misconceptions that have arisen about it.

One area of the Privacy Rule that was modified on August 14, which had been the subject of much public response during the comment period, was the requirement to obtain written consents from patients to use or disclose their protected health information to treat them, obtain payment, or carry out day-to-day operations. Requiring consent in these contexts would have been unnecessarily burdensome on patients and providers, and interfered with timely access to quality care, without improving privacy. It would have meant, for instance, that a doctor would have needed a patient to sign a privacy consent before he could use health information to treat that patient; that a specialist contacted by the patient's doctor would have needed to obtain the patient's consent to read treatment information; and that a pharmacist would have needed the patient's consent to fill a prescription written by the provider.

The Privacy Rule modifications removed the requirement that providers must obtain prior consent to use or disclose a patient's health information for treatment, payment or health care

operations purposes. While obtaining such consent is optional, this change assured that providers would have ready access to health information about their patients, and could readily share that information for treatment, for payment, and for health care operations so that timely access to quality health care would not be unduly impeded. At the same time, we strengthened the notice requirement by requiring direct treatment providers to make a good faith effort to obtain the patient's written acknowledgment that they received the notice. This ensures that a patient has the opportunity to consider the provider's privacy practices, both to be better informed of how their information may or may not be disclosed, and to be informed of their rights – which had been a primary goal of the consent requirement. Notably, the Privacy Rule retained the protections that give patients the right to decide whether to authorize uses or disclosures of their information for marketing purposes, or to employers.

Similarly, the modified Privacy Rule clarified that with reasonable safeguards, uses and disclosures that were merely incidental to appropriate Privacy Rule uses and disclosures would not constitute a violation of the Rule. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a result of another use or disclosure that is permitted by the Rule. The Privacy Rule recognizes that communications necessary for quick, effective and high quality health care might unavoidably lead to overheard communications. Thus, a physician may discuss a patient's condition or treatment regimen in the patient's semi-private room, and a pharmacist may discuss a prescription with a patient over the pharmacy counter, provided that reasonable precautions (such as lowered voices and/or talking apart from others) are employed.

Both of these examples demonstrate how the Privacy Rule, as modified, both protects patient information, but avoids imposing unnecessary impediments to quality health care.

Since April 14, 2003 there has been widespread compliance by health plans, health care clearinghouses, and those providers covered by the Privacy Rule ("Covered Entities"). For example, physicians, hospitals, clinics, pharmacies, health insurance carriers, employer group health plans and others have distributed Notices, required by the Privacy Rule, that tell consumers about how their health information can and cannot be used and disclosed, and their rights, including :

- the right to inspect and obtain a copy of the individual's protected health information;
- the right to amend or correct protected health information;
- the right to request restrictions on certain uses and disclosures of protected health information;
- the right to receive protected health information through confidential communications;
- the right to receive an accounting of certain disclosures of their protected health information;
- the right to receive a copy of the Notice of Privacy Practices; and
- the right to complain to a covered entity or to OCR if an individual believes a covered entity has breached the Privacy Rule.

Given the extensive scope of the protections established in the Privacy Rule, implementation has gone smoothly, without the disruption of the healthcare system that had been predicted in some quarters. This is due in part to the commitment made by the Office for Civil Rights and the Department to public education, a commitment that continues in various outreach efforts, voluntary compliance initiatives, and even in investigation of complaints. And it is due to the attention health care providers have given to the Rule and their efforts to implement it. As I will explain, OCR has produced a wide variety of guidance and technical assistance that is focused and prioritized as we discern the need for further clarification. These efforts have significantly contributed to reducing confusion and eliminating misconceptions that have been reported in these first months of compliance. In many of these areas, confusion appears to have arisen not because of problems with the Privacy Rule itself, but rather due to misconceptions about it. In addition, it appears that providers and other covered entities are also serving to educate their fellow covered entities where overly restrictive practices were initially being adopted and, incorrectly, blamed on the Privacy Rule.

For example, we have heard reports that some covered entities are reluctant to share health information with other providers, for the purpose of treating their patients, claiming that the Privacy Rule requires that patients execute written consents for these disclosures to occur. Providers who claim that this practice is mandated by the Privacy Rule are incorrect, and apparently are unaware

that the Rule was modified specifically to permit treatment disclosures among providers without the need for patient consent. In fact, the Privacy Rule allows doctors, nurses, hospitals, technicians, and other covered health care providers to use or disclose patient health information, including X-rays, laboratory and pathology reports, diagnoses, and other medical information for treatment purposes, without the patient's authorization. This includes sharing a patient's health information to consult with other providers, to treat a different patient, or to refer the patient to other providers.

Similarly, we have seen reports and heard from consumers, as you may have heard from your constituents, that providers cannot share information with family members, loved ones, friends, or others whom are identified by the individual as involved in their care or the payment for their care. Again, rather than foreclosing such communications, the Privacy Rule provides a number of common-sense methods which appropriately permit such disclosures while respecting and protecting an individual's right to control their health information. Under 45 CFR 164.510(b), the Privacy Rule specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient's care or payment for health care. Where the patient is present and has the capacity to make health care decisions, the covered entity may discuss this information with these individuals if the patient agrees or, when given the opportunity, does not object. The covered entity may also share relevant information with these individuals if it can reasonably infer, based on professional judgment, that the patient does not object. For example, if a patient brings a friend to a medical appointment and asks if the friend can come into the treatment room, her doctor can reasonably infer that the patient does not object. Under these circumstances, a doctor or plan can disclose any information that is directly relevant to the family member or friend's involvement with the patient's care, or payment related to the individual's care.

On a related point, this is also the section of the Privacy Rule that allows Congressional staffers to intercede with covered entities on behalf of your constituents who write in and ask your offices to help, for instance, in obtaining treatment, or with a payment question. As I mentioned earlier, where a patient identifies an individual as being involved in their care – as they might when writing to your office and seeking assistance in these matters -- the Privacy Rule permits covered

entities to share information directly related to that involvement in matters pertaining to the constituent's treatment or payment.

We have also heard reports – incorrect, again – that because of the Privacy Rule, hospitals can no longer maintain patient directories so that appropriate information can be provided to family members, loved ones, clergy or other members of the public who call to inquire about patients. Along similar lines, we have seen reports that clergy, in particular, can no longer visit members of their congregations in the hospital, because the Privacy Rule forbids clergy access to any information about hospitalized individuals, or to information about the individual's religious affiliation. Though it does not mandate that hospitals maintain such directories or make such disclosures, the Privacy Rule specifically provides and envisions that the common and helpful practice of maintaining such directories will continue. Consistent with the overall approach of the Rule, it lets individuals choose whether their information should be included in the facility directory, or to opt out. Even where, because of emergency or the individual's incapacity, the patient cannot be given the opportunity to opt out, the Privacy Rule allows the covered entity to determine, based on experience and professional judgment, whether including the information would be in the best interests of the patient. This information – including the patient's name, location in the hospital, and general description of the patient's condition) can be accessed by anyone inquiring about the patient by name.

Clergy similarly can access this information by asking for patients by name, of course; but the Privacy Rule also allows hospitals to include in the facility directory, and to disclose to members of the clergy, the religious affiliation of patients who have opted to provide it; and members of the clergy can obtain this information without having to inquire about specific patients by name. As with disclosures of information in facility directories to other members of the public, the patient (or those with appropriate authority to act on their behalf) will have the opportunity to decide whether they want their information included in the directory, or to opt out. If they elect to have the information included, then their loved ones, clergy, or others who inquire can have access to this information.

The misconceptions discussed here are among the most common we have heard. It appears that confusion on these issues is dissipating, as covered entities and consumers become more

familiar with the Rule's requirements. These problems do not arise because of the Privacy Rule, but rather seem to arise either because providers have elected to take a more restrictive approach than the Privacy Rule requires, or because of a misconception about the requirements of the Privacy Rule. To address this latter concern, OCR has conducted, and is continuing to conduct, an extensive public education effort to produce and disseminate a wide range of guidance about various aspects of the Rule that are of concern to the public and to covered entities. And we are pleased that the information we have disseminated is being well received.

Continuing extensive outreach efforts that we undertook in prior years, OCR senior Privacy experts, from Washington DC and throughout our regions, have made well over a hundred presentations during 2003 alone. These include four national, all-day HIPAA Privacy Rule conferences, attended by some 6000 participants, sponsored in conjunctions with universities and key industry groups, in February and March of this year, at which OCR and other Department experts in the Rule offered in-depth seminars and answered questions on all aspects of the Privacy Rule. In addition, OCR has conducted or participated in numerous telephone audio conferences. In one toll-free call arranged for by the Departments' Centers for Medicare and Medicaid Services and paid for by OCR, an estimated 8500 people participated on over 4000 telephone lines. Moreover, in conjunction with the Centers for Medicare and Medicaid Services (CMS), OCR offers a free call-in line, 1-866-627-7728 for HIPAA questions. If the trained operators are unable to answer the questions directly or by reference to resource materials and our website, they refer the caller to an OCR Privacy Rule specialist. Since April 1, combined phone-line operators and OCR staff have received and responded to some 14,000 calls related to the Privacy Rule. In many cases, we are gratified that the questions being raised are addressed by guidance materials posted on the OCR website, www.hhs.gov/ocr/hipaa. It is noteworthy that, in the first week of compliance, some 1334 calls were received by our HIPAA operators for Privacy related matters. But, perhaps as an indication that covered entities and consumers are becoming more familiar with the Privacy Rule, by the week ending September 13, 2003, the number of calls was down to 480, only about a third of the initial volume.

Our website plays a key role in our outreach activities, and has enabled us to post and broadly disseminate information that provides additional clarification in helpful areas, and to

clear up misconceptions when they arise. In turn, providers can use these posted materials to educate other providers who, for instance, believe that they cannot share treatment information with each other, without patient consent; it is also useful to patients and their loved ones who seek to correct the misconceptions of hospitals or other providers who mistakenly fail to grasp the latitude afforded by the Privacy Rule to share information with loved ones. From January through July 2003, OCR's Privacy Rule homepage received 847,800 visits.

We want to focus on the information available at this website since it offers a myriad of helpful information for consumers, and technical assistance for covered entities. [See Exhibit 1.] For instance, it includes:

- a comprehensive *Summary of the HIPAA Privacy Rule*, which is linked to other guidance on specific topics referenced in the *Summary*. It is an excellent means of obtaining a clear overview of the Privacy Rule, and finding more thorough information on particular topics;
- A *Covered Entity Decision Tool*, an interactive tool that provides extensive information to assist entities in determining whether they are covered by HIPAA
- Sample *Business Associate Contract Provisions*,
- extensive guidance on particular aspects of the Rule, including
    - General Overview
    - Incidental Uses and Disclosures
    - Minimum Necessary
    - Personal Representatives
    - Business Associates
    - Uses and Disclosures for Treatment, Payment and Health Care Operations
    - Marketing
    - Public Health
    - Research
    - Worker's Compensation Laws
    - Notice
    - Government Access

- the HHS National Institute of Health's Guide to Research, "*Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule*", with related information for Institutional Review Boards, and about Authorizations for research;
- the HHS National Institute of Health's Guide to Research, *"Authorizations for Research and Institutional Review Boards"*
- the Center for Disease Control's Guidance, *"HIPAA Privacy Rule and Public Health"*
- a fact sheet for consumers, *"How to File a Health Information Privacy Complaint"*
- a fact sheet for consumers, *"Protecting the Privacy of Patient's Health Information"*

A key feature of our website, accessed over 1.2 million times since January of this year is our database with over 200 searchable Frequently Asked Questions ("FAQs") (EXHIBIT 2). The database is simple to use, and provides clarifications on many different aspects of the Privacy Rule, including some of the areas that we have already discussed. For instance, there are a number of questions that address permissible disclosures for treatment and disclosures to clergy. In addition, we are in the process of posting additional Questions and Answers with guidance on informing visitors about a patient's location in a facility or a patient's general condition; and disclosures to family members.

Our website is also organized to be as helpful as possible. For instance, we include a link focused on materials we believe are of particular interest to small providers and small businesses.

Finally, we are developing additional targeted technical assistance materials, focusing on explaining the Privacy Rule to consumers as well as specific industry groups, required to comply with the Rule such as smaller health care providers, institutional health care providers, health plans, group health plans, health care clearinghouses, and state and local governments .

We are pleased that the industry has developed a better understanding of the Rule, in large part because of the workability changes we adopted last year, and the extensive guidance and FAQs we have published.

I also want to discuss our experience enforcing the Rule and the Department's enforcement posture. OCR has the authority to investigate complaints and it has authority to conduct reviews of covered entities for compliance with the Privacy Rule. As a practical matter, our efforts are primarily complaint-driven, though we have compliance review authority in case we become aware of a situation where no complaint has been filed, but which demands our attention. Any person can file a complaint with OCR, and in the first five months since the compliance date, we have received over 1800 complaints. We have already been able to resolve and close about 30% of those complaints, either because they did not raise a privacy issue, because the action complained of did not constitute a violation of the Rule, or because we were able to resolve the matter expeditiously and informally – through voluntary compliance – usually after providing some technical assistance.

The Privacy Rule provides that HHS will seek cooperation of covered entities in obtaining compliance and can provide technical assistance to covered entities to help them voluntarily comply with the Rule, even after investigations begin. OCR continues to encourage voluntary compliance from covered entities because it is often the quickest and the most efficient means of ensuring that individuals benefit from the protections in the Rule. Of course, even in instances where OCR is giving technical assistance, the responsibility for compliance remains with the covered entity. In appropriate circumstances Congress has provided that the Department may seek to impose civil penalties under the statute: civil penalties may not be imposed for Privacy Rule violations if the person did not know, and by exercising reasonable diligence would not have known, of the violation; or if failure to comply was due to reasonable cause and not willful neglect, and the entity corrects the violation within thirty days of when it knew or should have known of the error. While OCR continues to seek informal resolution through voluntary compliance wherever appropriate, and expects to be able to resolve the vast majority of cases through these informal means, it will employ the variety of enforcement

options available as needed to ensure that consumers receive the privacy protections afforded by the Rule.[3]

Finally, I would like to take a moment to address the costs associated with implementing the Privacy Rule, in which the Committee has expressed an interest. We estimated in the preamble to the December 2000 Rule that the Privacy Rule would produce compliance costs of $17.6 billion (with present value costs of $11.8 billion over ten years- 2003-2012). Subsequently, in adopting the August 2002 modifications, the Department estimated that improvements in workability in the modifications, which helped to avoid unintended consequences of the Privacy Rule, would lower the compliance cost of the Privacy Rule by approximately $100 million over ten years.

We also conducted a Regulatory Flexibility Analysis of the economic impact of the Rule on small entities, i.e., organizations with less than $5 million in annual revenues.[4] We noted in our assessment of the costs associated with compliance that the Privacy Rule is flexible and scalable, i.e., wherever possible, the Rule provides a covered entity with flexibility to create policies and procedures that are best suited to the entity's current practices in order to comply with the Rule's requirements. This approach allows covered entities to develop policies and practices that achieve the goal of protecting the privacy of individually identifiable health information, as set forth in the Rule, in a way that is most efficient for them. HHS adopted this scaled approach to minimize the burden on all entities, with an emphasis on small entities. We estimated in December 2000 that the total costs to small businesses of complying with the final rule in the initial year of 2003 would be $1.9 billion and that the ongoing costs to small business

[3]The Department of Justice is responsible for enforcement of HIPAA violations that are subject to criminal penalties.

[4]We assumed that small business in the health care sector affected by this Rule could include such businesses as: nonprofit health plans, hospitals, and skilled nursing facilities, small businesses providing health coverage, small physician practices, pharmacies, laboratories, durable medical equipment suppliers, health care clearinghouses, billing companies, and vendors that supply software applications to health care entities.

from 2004 to 2012 would be $9.3 billion; and we stated in August 2002 that the impact of the published modifications would be *de minimus* on small entities.[5]

HIPAA states that "[a]ny standard adopted under this part [i.e., all HIPAA administrative simplification provisions, including those related to uniform standards for Transactions and Code Sets] shall be consistent with the objective of reducing the administrative costs of providing and paying for health care." While Congress and the Department recognized and anticipated that implementation of the Privacy Rule would be accompanied by significant costs, as set forth above, it was also anticipated that these costs would be offset by efficiencies realized in other aspects of the Rule. In addition, the Department has sought – through adoption and modification of the Privacy Rule, through its public outreach and technical assistance, and through its approach to compliance – to accomplish two key goals: protecting the privacy of health information, while not erecting barriers that unduly impede access to quality health care.

The Office for Civil Rights and the Department have taken significant steps to help covered entities come into compliance with the Privacy Rule, and we are committed to continuing these efforts. We believe our efforts have contributed significantly to reducing the burden and the costs of compliance, and have helped to clarify misconceptions that have arisen with respect to the Privacy Rule. The Department recognizes, as it always has, that significant costs would be associated with achieving the protections and safeguards called for in the Privacy Rule, but we continue to believe that efficiencies to be realized through Administrative Simplification will outweigh these costs. Even so, the Department and OCR are working diligently to ease these costs through our extensive public outreach and technical assistance efforts, through our emphasis on voluntary compliance efforts in all appropriate circumstances. We believe these efforts are accomplishing the goals highlighted by Secretary Thompson when announcing final modifications to the Privacy Rule a year ago: providing a foundation of federal protection for the privacy of health information, while not impeding access to quality health care.

Thank you for this opportunity to address the committee. I look forward to the opportunity to respond to your questions.

---

[5]In addition, in our December 2000 Rule, we estimated that the total federal costs under this Rule would be approximately $196 million in 2003 and $1.8 billion over ten years.